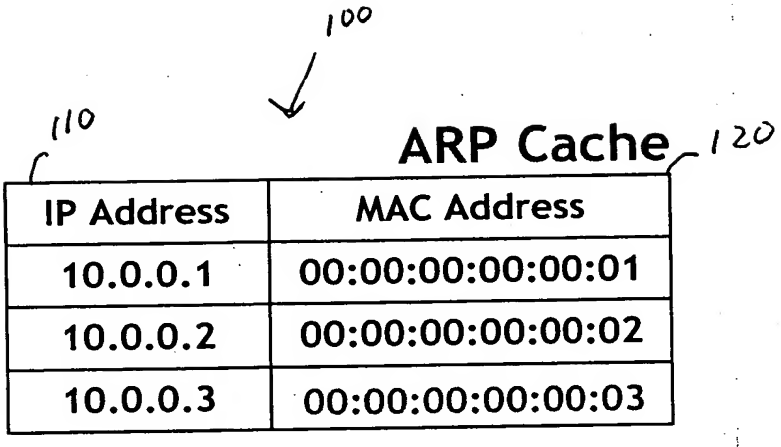

FIG. 1 (prior art)

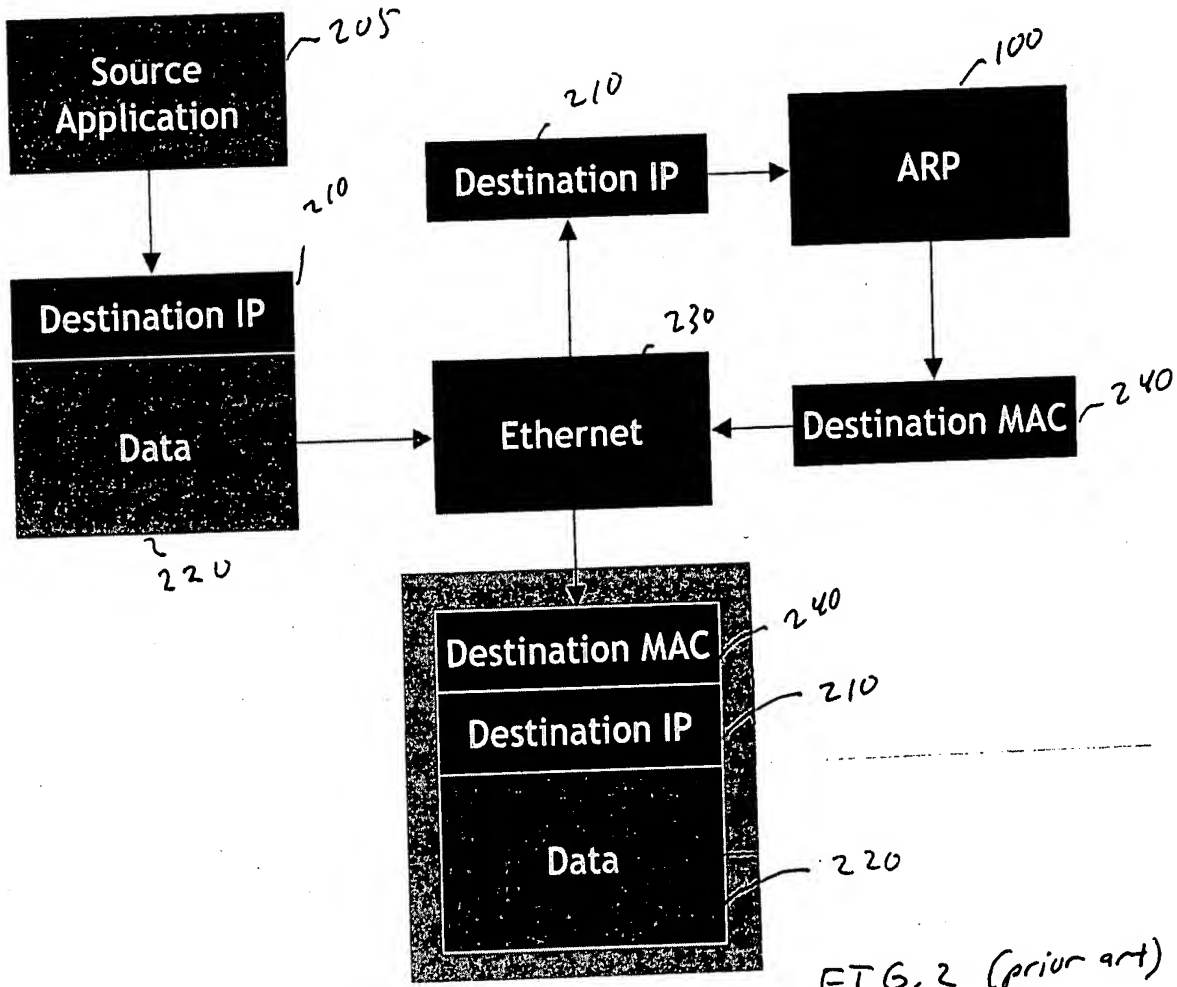

FIG. 2 (prior art)

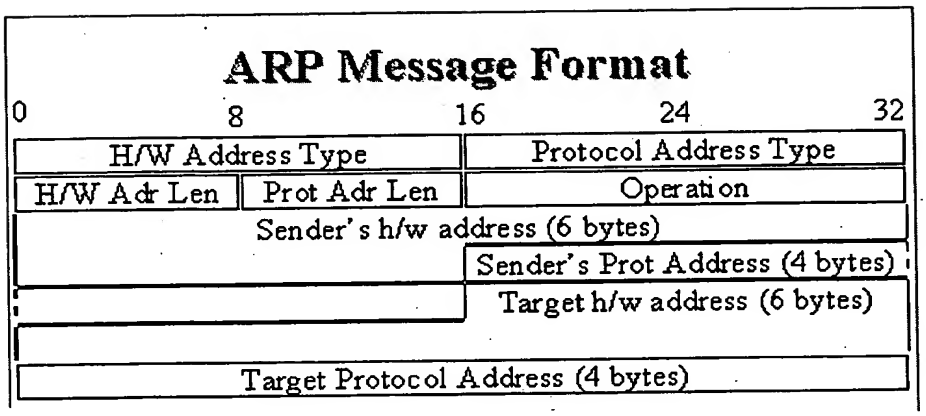

FIG. 3 (prior art)

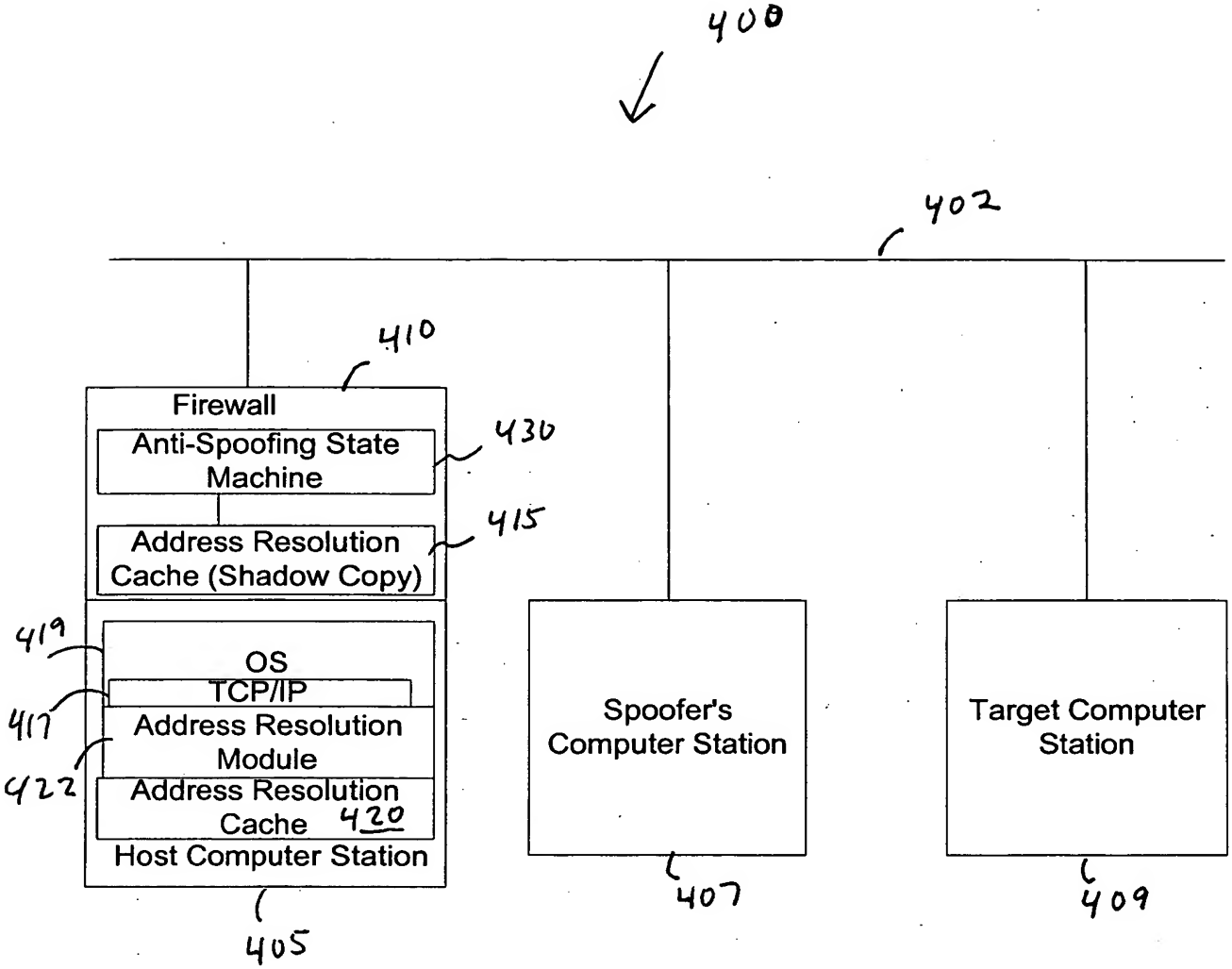
400
402
410
Firewall
Anti-Spoofing State Machine
430
Address Resolution Cache (Shadow Copy)
415
419
OS
TCP/IP
417
Address Resolution Module
422
Address Resolution Cache 420
Host Computer Station
405
Spoofer's Computer Station
407
Target Computer Station
409

FIG. 4

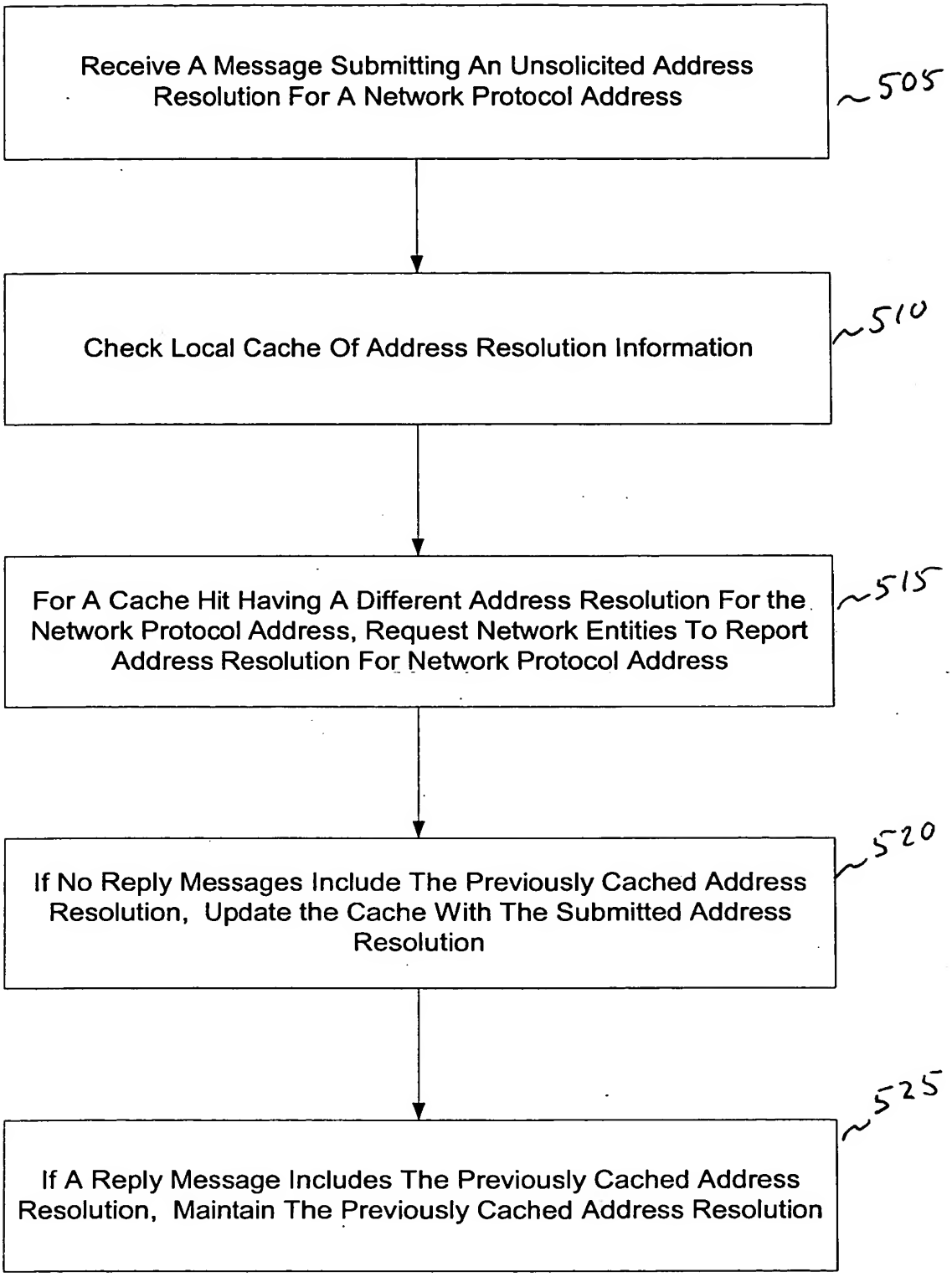
Receive A Message Submitting An Unsolicited Address Resolution For A Network Protocol Address
505
Check Local Cache Of Address Resolution Information
510
For A Cache Hit Having A Different Address Resolution For the Network Protocol Address, Request Network Entities To Report Address Resolution For Network Protocol Address
515
If No Reply Messages Include The Previously Cached Address Resolution, Update the Cache With The Submitted Address Resolution
520
If A Reply Message Includes The Previously Cached Address Resolution, Maintain The Previously Cached Address Resolution
525

FIG. 5

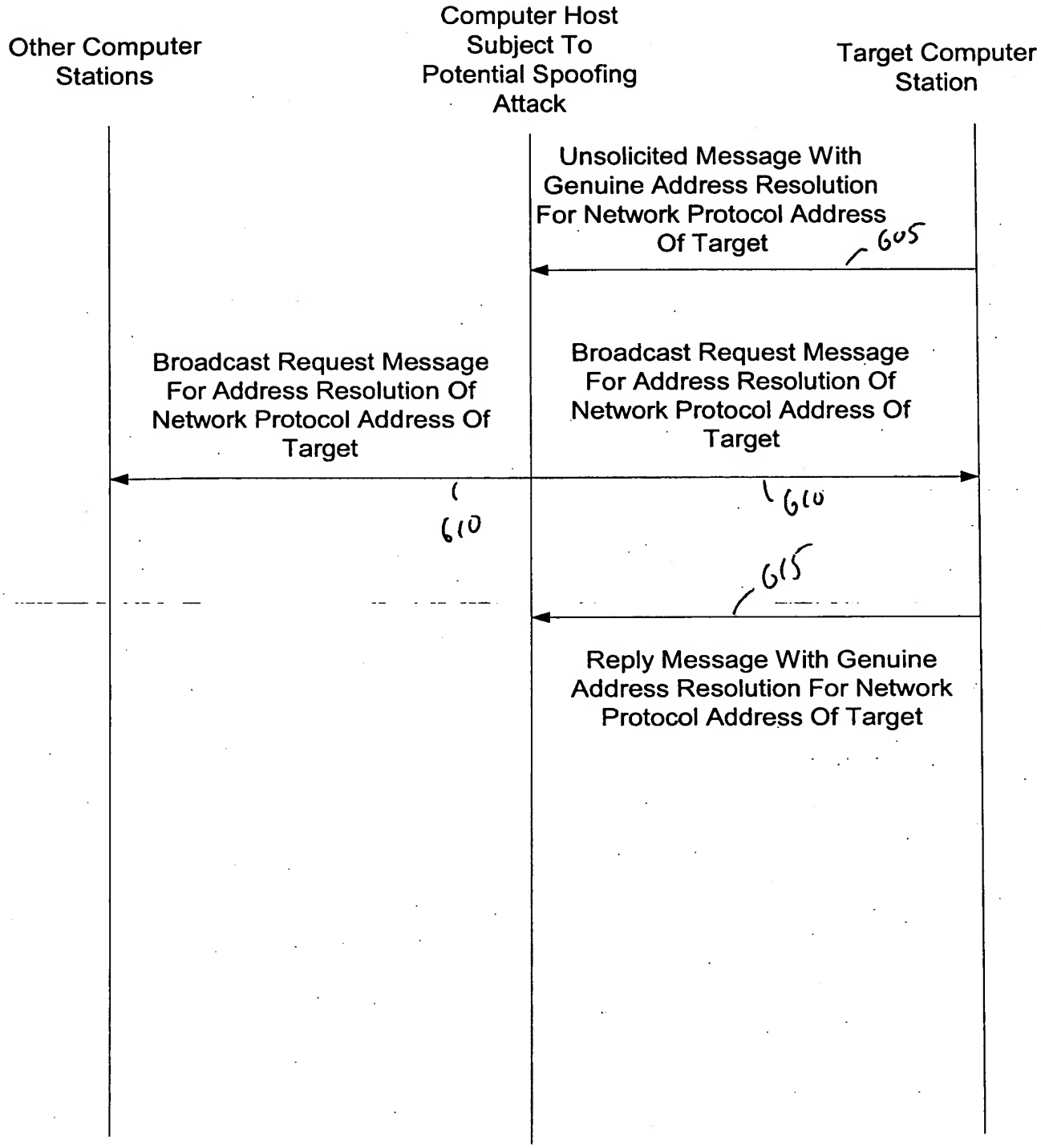
Other Computer Stations
Computer Host Subject To Potential Spoofing Attack
Target Computer Station
Unsolicited Message With Genuine Address Resolution For Network Protocol Address Of Target
605
Broadcast Request Message For Address Resolution Of Network Protocol Address Of Target
Broadcast Request Message For Address Resolution Of Network Protocol Address Of Target
610
610
615
Reply Message With Genuine Address Resolution For Network Protocol Address Of Target

FIG. 6

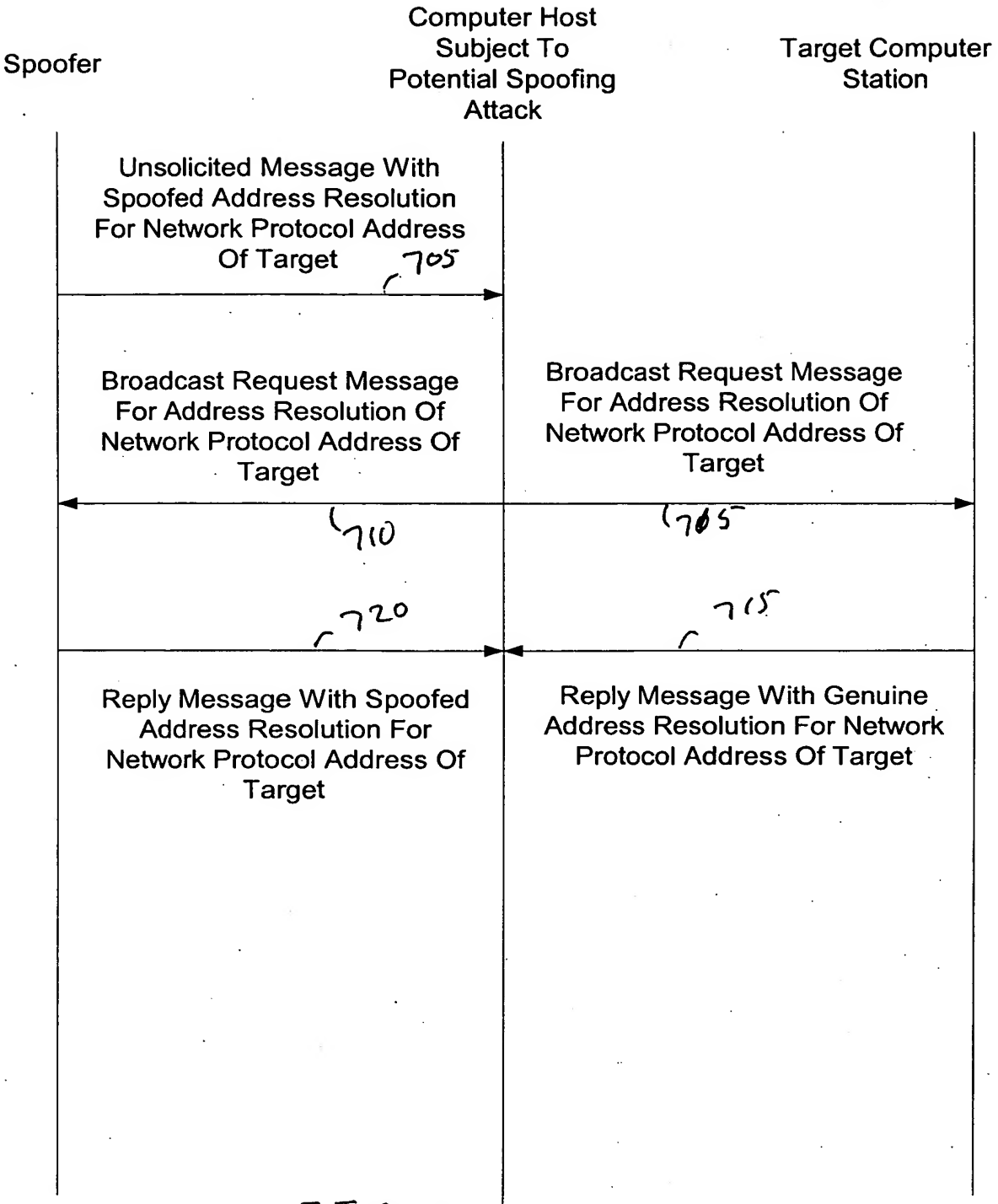
Spoofer
Computer Host Subject To Potential Spoofing Attack
Target Computer Station
Unsolicited Message With Spoofed Address Resolution For Network Protocol Address Of Target
705
Broadcast Request Message For Address Resolution Of Network Protocol Address Of Target
Broadcast Request Message For Address Resolution Of Network Protocol Address Of Target
710
705
720
715
Reply Message With Spoofed Address Resolution For Network Protocol Address Of Target
Reply Message With Genuine Address Resolution For Network Protocol Address Of Target

FIG. 7